

Exhibit 15

PUBLIC

Alphabet Inc. Response to Questionnaire on Electronically Stored Information

This response reflects currently available information and is intended to provide an overview of the issues requested by the U.S. Department of Justice (DOJ), and to act as a supplement to the numerous discussions the parties have had to date. Google's investigation is ongoing and Google will supplement this response as needed.

I. Definitions and Instructions

A. "ESI" means electronically stored information as the term is used in the *Federal Rules of Civil Procedure*.

B. All responses should include all systems, practices, and procedures used at any time during the period specified in the Second Request/CID/Subpoena that may contain potentially responsive information.

C. All responses should reflect an inquiry into actual employee practices, and not just the organization's policies.

D. The term "archive" means long-term storage repositories for data, often for purposes of historical reference, and denotes a distinct concept from a "backup," which is created in order to restore data if needed at a later date (e.g., for disaster recovery).

II. Background

Provide:

A. current organizational charts for your organization's information technology ("IT") unit;

Google response: As we have discussed, Google does not keep traditional organizational charts in the ordinary course of business. Google also does not maintain a traditional IT department as Google largely operates on the same systems and software designed and maintained by Google for customers and partners. Traditional IT functions are largely provided by various units within Google. Google "Techstop" (over 450 employees) provides Google's internal technical support, including provisioning hardware and troubleshooting hardware issues. The Corporate

Engineering (Corp Eng) unit (approximately 2,500 employees) is responsible for building, implementing, and supporting Google's internal tools and systems, such as ticketing systems and employee performance reviews. Google also has a small Corporate Cloud Operations (Corp Cloud Ops) unit to manage internal issues related to G Suite and Gmail for Google employees. Some electronic discovery functions are managed in-house by Google's Discovery Operations unit. In response to the DOJ's request during our November 20, 2019 call, Google will identify the top-level employee and their direct reports for Techstop, Corporate Cloud Operations, and Discovery Operations.

B. written policies related to document retention and management, along with the period in which the policy was in effect and whether the policy is enforced and by whom; and

Google response: Google has two primary written policies related to document retention, attached as Annexes A (General) and B (Gmail) to this response. These policies govern retention of e-mail, general documents, legal holds and other topics. These policies have been in place since 2013.

C. a description of IT functions performed by outside contractors.

Google response: Core informational technology functions, such as servers and storage are generally handled by Google. Some limited tasks, such as laptop deployment, may be supplemented by third-party vendors in the Techstop unit.

III. Computer Hardware and Systems

Describe the computer hardware and systems used in the conduct of your organization's business, addressing:

A. the kinds of computers used (*e.g.*, mainframe, work stations, desktops, laptops, tablets, and any other portable devices);

B. the types and versions of all operating systems used (*e.g.*, Windows, Linux, UNIX), including dates of major changes or upgrades;

C. the types of servers used (*e.g.*, Exchange servers), the approximate number of each server type, and the physical locations of servers;

D. use of desktops, including where business information is saved and

backed-up on the desktops, how the desktops are connected to the network (*e.g.*, LAN), and any use for telecommuting;

E. use of company laptops, tablets, or other handheld or portable digital devices (*e.g.*, smartphones, BlackBerry devices, Apple iPads) to conduct business, where business information is accessed, saved or backed-up on the company devices, how the devices are connected to the network (*e.g.*, remote access programs, synchronization procedures), any use for telecommuting, and whether the devices contain business-related messages (including SMS or PIN), documents, or information not stored on the network;

F. use of employees' own personal laptops, tablets, or other handheld or portable digital devices (*e.g.*, smartphones, BlackBerry devices, Apple iPads), how these devices are connected to your organization's network (*e.g.*, remote access, web access), where work-related ESI is saved or backed-up for the personal devices, any use for telecommuting, and whether they contain business-related messages (including SMS or PIN), documents, or information not stored on the network;

G. use of removable storage media (*e.g.*, thumb drives, CDs, external hard drives);

H. all third-party storage locations containing ESI created by your organization (*e.g.*, ASPs, cloud computing, external host servers);

I. all legacy systems containing ESI not migrated to current systems; and

J. where, and for how long, ESI created by former employees is stored.

Google response: Google employees use a variety of machines, including laptops, desktops, and tablets. Employees can generally choose between machines that operate on either Chrome OS, Mac OS, Linux and Windows. Google's servers are spread out across the world. Employees can typically choose to have a company-issued mobile device or "Bring Your Own Device" (for mobile devices) as long as the BYOD is set up with appropriate security protocols. Google employees usually access various cloud-based productivity solutions to conduct business (*e.g.*, G Suite for e-mail, document creation, and document storage; G3 for source code work). Most of these applications are developed by Google. ESI from former employees is stored consistent with the retention policies in Annexes A and B. E-mails from former employees (who are not on a legal hold) are subject to the same retention policies as regular employees.

IV. Applications and Information Management Software

Describe the applications and information management software used in your organization's business, addressing:

A. E-mail and Other Electronic Communication Software

1. e-mail programs (including version) (*e.g.*, Microsoft Outlook, web-based e-mail accounts) and any related applications used (*e.g.*, contacts, calendar, notes, tasks);

Google response: Google primarily uses the Google-developed "G Suite" solution for workplace productivity. G Suite is a cloud-based system that includes email (Gmail), chats (Hangouts/Hangouts Chats), storage/management (Drive), and other productivity applications (*e.g.*, Sheets, Slides, Docs).

2. where e-mails are stored (*e.g.*, on network servers, local drives, web or cloud-based);

Google response: E-mails are systematically stored in the cloud.

3. limits on e-mail retention (*e.g.*, size of mailbox, length of retention), and when such limits were put into effect;

Google response: There are no limits on the size of mailboxes. Consistent with Google's retention policy in Annex B, e-mails are generally retained for a period of 18 months with some exceptions (*e.g.*, e-mails marked as unread are auto-deleted after 6 months, a legal hold puts e-mail on hold until the legal hold is lifted, and e-mails can be marked for indefinite retention by the user).

4. whether routine journaling occurs, the system or program used, where journaled e-mails are stored, and the length of time journaled e-mails are normally maintained;

Google response: Google does not use routine journaling.

5. whether e-mails are routinely deleted (or auto-deleted) and the schedule or parameters for such deletions;

Google response: Consistent with Google's retention policies, e-mails marked as read e-mails are auto-deleted after a period of 18 months and e-mails marked as unread are auto-deleted after a period of 6 months, from the perspective of the user, unless they are marked for retention due to a litigation hold or other reason. The retention period applies to the entire e-mail thread and is measured from the timestamp of the most recent e-mail in the thread.

6. how e-mails are accessed remotely;

Google response: G Suite is cloud-based and therefore all of the productivity applications that reside in G Suite, including Gmail, are accessed via a browser or phone app.

7. use of text or other messaging applications including Instant Messaging ("IM") programs, and the period for which these messages are retained;

Google response: G Suite has messaging capabilities, including Google Hangouts. Google Hangouts messages are generally retained for a period of 30 days if they have been marked on-the-record, and potentially longer if on-the-record messages are on legal hold.

8. any voicemail or unified messaging system used, the programs used for voicemail retention, how long voicemails are retained, whether voicemail messages are migrated to another electronic system, *e.g.*, email, and the format in which voicemail is stored (*e.g.*, .wav, etc.); and

Google response: Google does not maintain a unified voicemail messaging system. Google employees have access to voicemail through their mobile device, which, as described above, may be company-issued or BYOD. Voicemails are stored locally on a mobile device and are subject to deletion based on how an employee has configured their device settings. Some Google employees use Google Voice (including voicemails).

9. any audio recording system used, the programs used for retention of recordings, the data tracked by each program or system, how long recordings are retained, whether recordings are migrated to another electronic system, and the format in which recordings are stored (*e.g.*, .wav, etc.).

Google response: Google does not generally make any systematic use of employee audio recordings.

B. Other Applications

1. each application (including version) used to create ESI, including word processing, spreadsheet, presentation, financial and accounting, and any customized or proprietary software applications; and
2. where ESI created through such programs is stored, and whether each such storage space is shared or personal.

Google response: Google uses G Suite as its primary business software, including word processing, spreadsheets, presentations, and other uses.

C. Document Management

1. each document management application (including version) (*e.g.*, eFileCabinet, DocuWare, LogicalDOC) used;
2. the types of ESI stored using such programs; and
3. where such ESI is stored.

Google response: As described above, e-mail and other employee documents (*e.g.*, spreadsheets, presentations) are typically created and stored using applications within G Suite.

V. Internet, Intranet, and Other Web-based Information

A. Describe the internet and intranet sites that your organization maintains, addressing:

1. the type of information maintained on each site;
2. which groups or categories of users (not lists of names of individuals) have rights to add, delete, or alter data on each site;
3. where each site is stored;
4. whether ESI contained in each database is routinely deleted (or

auto-deleted) and the schedule or parameters for such deletions; and

5. any approval process or procedures to alter content on each site.

Google response: Google maintains a number of different websites, which are easily accessible at Google.com.

Google does not maintain a single intranet repository. There are several internal documentation sources to which employees have access like Drive, Sites, and wikis. Other internal-facing resources include Google3 (coding repository), structured databases (such as Ghire, Spanner, BigQuery), and tickets systems. Some Google employees also use third-party tools such as Salesforce and Workday.

Internal sites can be created by any Google employee to include any type of information.

B. Describe the web-based services your employees or the organization use in relation to your organization's business, addressing:

1. which, if any, social networking sites (*e.g.*, Facebook, MySpace, Twitter, LinkedIn), personal e-mail accounts (*e.g.*, Hotmail, Gmail), collaborative work environments (*e.g.*, wikis, SharePoint, blogs, WebEx), video or photo sharing sites (*e.g.*, YouTube, Flickr, Snapfish, etc.), web content management systems (*e.g.*, Drupal), chat services or software, or cloud storage or file sharing services (*e.g.*, Dropbox, Google Drive) are used;
2. how employees use each web-based service;
3. which groups or categories of users (not lists of names of individuals) have rights to add, delete, or alter data in each web-based service;
4. any approval process or procedures to alter content on any web-based services;
5. where the information for each web-based service is stored;
6. whether ESI contained in each web-based service is routinely deleted (or auto-deleted) and the schedule or parameters for such

deletions; and

7. the terms or provisions for the company's access to and copying of ESI in the service provider's possession.

Google response: As explained above, Google employees primarily use internal web-based services under the G Suite umbrella, including Gmail and Google Drive. The information for these services is stored in the cloud and the information is subject to Google's retention policies.

C. Identify any data room or temporary document repositories (*e.g.*, due diligence rooms).

Google response: Google Drive is the primary storage tool for Google employees' documents. In some limited cases, such as M&A due diligence, Google uses data rooms.

VI. Databases

Describe databases used in the conduct of your organization's business, addressing:

- A. the name of each such database and its underlying software (including version);
- B. the type of information each database contains;
- C. which groups or categories of users (not lists of names of individuals) have rights to add, delete, or alter data in each database;
- D. where each database is stored;
- E. whether ESI contained in each database is routinely deleted (or auto-deleted) and the schedule or parameters for such deletions; and
- F. the availability of regular or standard reports, data dictionaries, manuals, and training materials for each database.

Google response: Per our ongoing discussions, including our November 19, 2019 call, we continue to work on providing you with information regarding potentially relevant databases.

VII. Disaster Recovery Backup and Archiving Procedures

A. For each repository of ESI identified in response to this questionnaire, describe your organization's backup procedures, addressing:

1. the types of backups performed (*e.g.*, full backups, incremental backups, redundant systems);
2. the types of data backed up (*e.g.*, e-mails, word processing documents);
3. the backup schedule (*e.g.*, each business day, weekly, and monthly);
4. the period for which ESI contained on backups may be restored (*i.e.*, the number of months or years backup media are retained before being overwritten);
5. whether backup media are individually labeled by type of data stored on the media, or by employees whose data is stored on the tape;
6. whether an individual e-mail account can be restored or the files of a single custodian restored, without restoring the entire backup media;
7. whether backup media are indexed and/or logged by backup software;
8. the type of media on which the backup data is stored, and the backup application (including version) used;
9. the use of any remote or on-line backup service;
10. the specific geographic location of any and all backup media, whether on or off-site;
11. whether backup media have been restored within the last two years, for any purpose, including for other litigation or to retrieve data inadvertently deleted from computer systems;

12. the cost associated with restoring one backup media component (e.g., one backup tape, restoring a user's mailbox, or a shared directory); and

13. the company's disaster recovery procedures.

B. Do the backups or archives contain ESI outside of your normal procedures? (For example, in relation to a merger, acquisition, or sale of assets or a business line, in relation to the migration of ESI from one system to another, or in relation to a major system upgrade.) If so, describe what was backed up or archived and whether it has been retained.

Google response: The extent to which a file is backed up is dependent on a number of factors, such as file type, date of creation, and date of deletion. Our regular retention periods for Drive and Gmail data is set forth in response to Question No. IV.

VIII. Preservation Efforts

Describe the actions that have been undertaken to preserve ESI potentially responsive to the Second Request/CID/Subpoena and when the actions were taken, addressing:

A. the steps taken to preserve responsive electronic documents, including:

1. issuing preservation notices to employees, contractors, and third parties;
2. the suspension of backup media recycling and overwriting; and discontinuation of auto-delete functions;

B. the preservation of potentially responsive ESI within computer systems, applications, document management software or systems, web-based information and systems, databases, servers, local drives attached to PCs, laptops, personal devices used by employees to conduct business, backup media, archival media, handheld devices, removable media, and other systems identified in response to this questionnaire;

C. the individuals covered, including contractors and third parties;

D. the time period covered; and

E. efforts to preserve ESI on a going-forward basis.

Google response: Google has put a legal hold in place. The legal hold suspends auto-deletion. Documents, including version history, are preserved as of the collection date. The hold notice also instructs custodians to preserve relevant documents.